

網路安全練習主機與電文資訊

```
主機URL: "http://class.softarts.cc/AppSecurity/encryptData.json"
Package 加密 Key: "zaq1xsw2cde3vfr4"
Password 加密 Key Prefix: "1qaz2wsx"
```

Exception Domains 設定 Key 值

```
NSEExceptionAllowsInsecureHTTPLoads
NSIncludesSubdomains
```

UDID登記表

[UDID登記表](#)

Data+RNCrypt.swift (0811 1450)

```
//
//  Data+RNCryptor.swift
//  HelloMySecureApp
//
//  Created by Kent Liu on 2018/8/11.
//  Copyright © 2018年 SoftArts Inc. All rights reserved.
//

import Foundation
import RNCryptor

extension Data {
    func decrypt(key: String) -> Data? {
        // Convert base64 encoded data to original data
        guard let encryptedData = Data(base64Encoded: self) else {
            print("Fail to convert base64 to data.")
            return nil
        }
        guard let decryptedData = try? RNCryptor.decrypt(data: encryptedData,
withPassword: key) else {
            assertionFailure("Fail to decrypt.")
            return nil
        }
        return decryptedData
    }
    func decryptToString(key: String) -> String? {
        guard let data = decrypt(key: key) else {
            return nil
        }
        let string = String(data: data, encoding: .utf8)
        return string
    }
}
```

```
        }
        guard let string = String(data: data, encoding: .utf8) else {
            print("Fail to convert data to string.")
            return nil
        }
        return string
    }
}
```

DataProtection練習憑證

僅支援有登記UDID的裝置. [憑證下載](#)

Bundle ID: com.kent.dataprotectiondemo
P12密碼: 1qaz2wsx

假 Pinning Hash

```
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
"BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="
```

main.swift 預設內容

```
import Foundation
import UIKit

autoreleasepool {
    UIApplicationMain(
        CommandLine.argv,
        UnsafeMutableRawPointer(CommandLine.unsafeArgv)
            .bindMemory(
                to: UnsafeMutablePointer<Int8>.self,
                capacity: Int(CommandLine.argv)),
        nil,
        NSStringFromClass(AppDelegate.self) //Or your class name
    )
}
```